Bernoullis Tafelrunde

Graduate Student Seminar

Monday, 22 May 2023, 12:15-13:00
Seminarraum 05.002, Spiegelgasse 5

Semira Einsele

Freie Universität Berlin

Gröbner Bases as a Tool in Cryptology

Abstract

Cryptography relies on mathematical foundations to ensure the security and integrity of sensitive information. Cryptanalysis, on the other hand, focuses on breaking encryption and uncovering vulnerabilities within cryptographic systems. In this talk, we discuss the important role of Gröbner bases in cryptanalysis. We begin by motivating the need to study polynomial systems in cryptology. Next, we analyze the multivariate division algorithm and highlight the issues that arise when a monomial ordering is absent. We then introduce Gröbner bases and demonstrate how they serve as a powerful tool in cryptanalysis.